CLAIMS

1. An authentication method for a distributed data processing environment in which a server data processing system has access to a repository storing cipher-protected client passwords, the cipher-protected client passwords having been generated by applying a cipher function to the client passwords, the method comprising:

a process at the client data processing system applying the cipher function to the client password which corresponds to the stored cipher-protected client password, thereby to generate a cipher-protected client password which is equivalent to the stored cipher-protected client password;

performing an authentication check using the client data processing system's cipher-protected client password and the server data processing system's stored cipher-protected client password as a shared secret for said authentication check.

2. A method according to claim 1, wherein the authentication check includes performing a mutual challenge-response authentication protocol check.

3. A method according to claim 1, wherein the cipher function is an encryption algorithm.

4. A method according to claim 3, wherein the authentication check comprises generating a common secret session key at both the client and server data processing systems, using the generated encrypted client password at the client and the stored encrypted client password at the server, and using this common secret session key in a mutual challenge-response authentication protocol.

5. A method according to claim 4, wherein the common secret session key is generated by applying a cipher function to each of the generated encrypted client password at the client and the stored encrypted client password at the server.

6. A method according to claim 1, wherein the cipher function is a hash function.

7. A method according to claim 1, wherein each cipher-protected client password stored in the repository is stored together with a respective token, and the cipher-protected client passwords are generated by

combining the client passwords with the respective token and applying the cipher function to the combination, and wherein the method includes:

a process at the server data processing system retrieving from the repository the respective token for a stored cipher-protected client password, and transmitting the token to a client data processing system; and

the process at the client data processing system applying the cipher function to the combination of the transmitted token and the client password which corresponds to the stored cipher-protected client password, thereby to generate the equivalent cipher-protected client password for use as a shared secret.

8. A method according to claim 7, wherein the token is a random number.

9. A method according to claim 1, wherein the server data processing system's password repository is preferably integrated within the operating system of the server data processing system.

10. method according to claim 9, wherein the operating system is an operating system conforming to the UNIX

operating system standard or derived from a UNIX conforming operating system.

11. A method according to claim 10, wherein the encryption algorithm is provided by the UNIX crypt() function.

12. An authentication method for a distributed data processing environment in which a server data processing system has access to a repository storing cipher-protected client passwords, each cipher-protected client password being stored together with a respective token, the cipher-protected client passwords having been generated by combining the client passwords with the respective token and applying a cipher function to the combination, the method comprising:

a process at the server data processing system retrieving from the repository the respective token for a stored cipher-protected client password, and transmitting the token to a client data processing system;

a process at the client data processing system applying the cipher function to the combination of the transmitted token and the client password which corresponds to the stored cipher-protected client password, thereby to generate a cipher-protected client password which is

equivalent to the stored cipher-protected client password; and

using the client data processing system's cipher-protected client password and the server data processing system's stored cipher-protected client password as a shared secret for a mutual challenge-response authentication check.

13. A computer program product comprising program code recorded on a machine-readable recording medium, wherein the program code includes a server process for participating in a mutual challenge-response authentication protocol, the server process having access to a repository storing a cipher-protected copy of client passwords, the cipher protected client passwords having been generated by applying a first cipher function to the client passwords, the server process comprising:

means, responsive to a client process indicating a requirement for an operation to be performed, for generating a server challenge and for transmitting the server challenge to the client process, thereby to enable the client process:

(i) to generate a cipher-protected client password by applying said first cipher function to the

client's password, thereby to provide the client and server processes with a shared secret; and then

(ii) to generate a client response and counter-challenge, the client response and counter-challenge including a message authentication code computed using the cipher-protected client password, and to forward it to the server process;

means for receiving the client response and counter-challenge from the client process;

means for accessing the repository and retrieving said stored cipher-protected client password;

means for generating, using said stored cipher-protected client password, a message authentication code corresponding to an anticipated client response and counter-challenge, and for comparing the received and generated message authentication codes to determine whether they match;

means, responsive to a match, for generating a server response to the client response and counter-challenge; and

means for forwarding the server response to the client process to enable the client process to perform an authentication check.

14. A computer program product, comprising program code recorded on a machine-readable recording medium, wherein the program code includes a client process for participating in a mutual challenge-response authentication protocol, the client process comprising:

means for indicating to a server process a requirement for an operation to be performed, thereby prompting the server process to generate and send a server challenge to the client process;

means for applying a cipher function to the client's password to generate a cipher-protected client password;

means, responsive to receipt of the server challenge, for generating a client response and counter-challenge, the client response and counter-challenge including a message authentication code computed using the cipher-protected client password;

means for forwarding the client response and counter-challenge to the server process, thereby to prompt the server process to:

(i) receive the client response and counter-challenge;

(ii) access a repository storing a cipher-protected client password, generated by applying said cipher

function to the client's password, to retrieve said stored cipher-protected client password;

(iii) generate, using said stored cipher-protected client password, a message authentication code corresponding to an anticipated client response and counter-challenge;

(iv) compare the received and generated message authentication codes to determine whether they match and, responsive to a match, to generate a server response to the client response and counter-challenge and to forward the server response to the client process;

wherein the client process also includes:

means for generating a message authentication code corresponding to an anticipated server response,

means for receiving the forwarded server response, and

means for comparing the forwarded and anticipated server responses to determine whether they match.

15. A data processing system including:

a repository storing a cipher-protected copy of client passwords, the cipher-protected client passwords having been generated by applying a first cipher function; and

a server process for participating in a mutual challenge-response authentication protocol with a client process having an associated client password, the server process comprising:

means, responsive to a client process indicating a requirement for an operation to be performed, for generating a server challenge and for transmitting the server challenge to the client process, thereby to enable the client process:

(i) to generate a cipher-protected client password by applying said first cipher function to the client's password, thereby to provide the client and server processes with a shared secret; and then

(ii) to generate a client response and counter-challenge, the client response and counter-challenge including a message authentication code computed using the cipher-protected client password, and to forward it to the server process;

means for receiving the client response and counter-challenge from the client process;

means for accessing the repository and retrieving said stored cipher-protected client password;

means for generating, using said stored cipher-protected client password, a message authentication code corresponding to an anticipated client response and counter-challenge, and for comparing the received and generated message authentication codes to determine whether they match;

means, responsive to a match, for generating a server response to the client response and counter-challenge; and

means for forwarding the server response to the client process to enable the client process to perform an authentication check.

16. A distributed data processing system comprising a first data processing system according to claim 14 and a client data processing system, the client data processing system including a client process for:

generating a cipher-protected client password by applying said first cipher function to the client's password, thereby to provide the client and server processes with a shared secret;

generating a client response and counter-challenge to the server challenge, the client response and

counter-challenge including a message authentication code computed using the cipher-protected client password;

forwarding the client response and counter-challenge to the server process;

receiving the forwarded server response;

generating an anticipated server response and comparing the received and anticipated server responses to determine whether they match; and

in response to a positive match, confirming successful authentication.